How to Stay Anonymous Online with Parrot Security OS

Parrot Security OS Overview

Parrot Security OS is a Debian-based Linux distribution designed for security testing, privacy, and anonymity. This tutorial covers essential tools and techniques for maintaining online anonymity.

Table of Contents

01 Initial Setup & Configuration

02 Network Anonymity with Tor

03 Anonymous Browsing

04 Encrypted Communications

05 Metadata Removal

06 VPN Configuration

07 Best Practices

1. Initial Setup & Configuration

System Hardening

1

Disable IPv6

(prevents IP leaks):

```
sudo sysctl -w
net.ipv6.conf.all.disable_ipv6=1
sudo sysctl -w
net.ipv6.conf.default.disable_ipv6=1
```

2

Enable MAC Address Randomization

```
sudo macchanger -r wlan0
```

Replace wlan0 with your network interface name.

3

Update System Regularly

```
sudo parrot-upgrade
```

2. Network Anonymity with Tor

AnonSurf - System-Wide Tor Routing

Parrot includes **AnonSurf**, which routes all traffic through Tor.

Start AnonSurf:

```
sudo anonsurf start
```

Check Status:

```
sudo anonsurf status
```

Change Tor Identity:

```
sudo anonsurf changeid
```

Stop AnonSurf:

```
sudo anonsurf stop
```

Enable on Boot (optional):

```
sudo systemctl enable anonsurf
```

Tor Browser

For web browsing, use the included **Tor Browser** instead of system-wide Tor when possible (better isolation).

Launch from: Applications → Internet → Tor Browser

3. Anonymous Browsing

Browser Configuration

Use Tor Browser with these settings:

- Set security level to "Safest" (shields icon → Advanced Security Settings)
- Disable JavaScript for maximum anonymity
- Never maximize window (prevents fingerprinting)
- Clear cookies after each session

Firefox Hardening (if not using Tor Browser):

- Install uBlock Origin and Privacy Badger
- Disable WebRTC: about:config → set media.peerconnection.enabled to false
- Use HTTPS Everywhere
- Disable geolocation, camera, and microphone

DNS Leak Prevention

Use Tor DNS or encrypted DNS:

```
# Edit resolv.conf
sudo nano /etc/resolv.conf
```

Add:

```
nameserver 127.0.0.1
```

Or use DNSCrypt:

```
sudo systemctl enable dnscrypt-proxy
sudo systemctl start dnscrypt-proxy
```

4. Encrypted Communications

Email - Thunderbird with GPG

Generate GPG Key:

```
gpg --full-generate-key
```

List Keys:

```
gpg --list-keys
```

Export Public Key:

```
gpg --armor --export [your-email@example.com](mailto:your-email@example.com) > publickey.asc
```

Encrypt Email in Thunderbird:

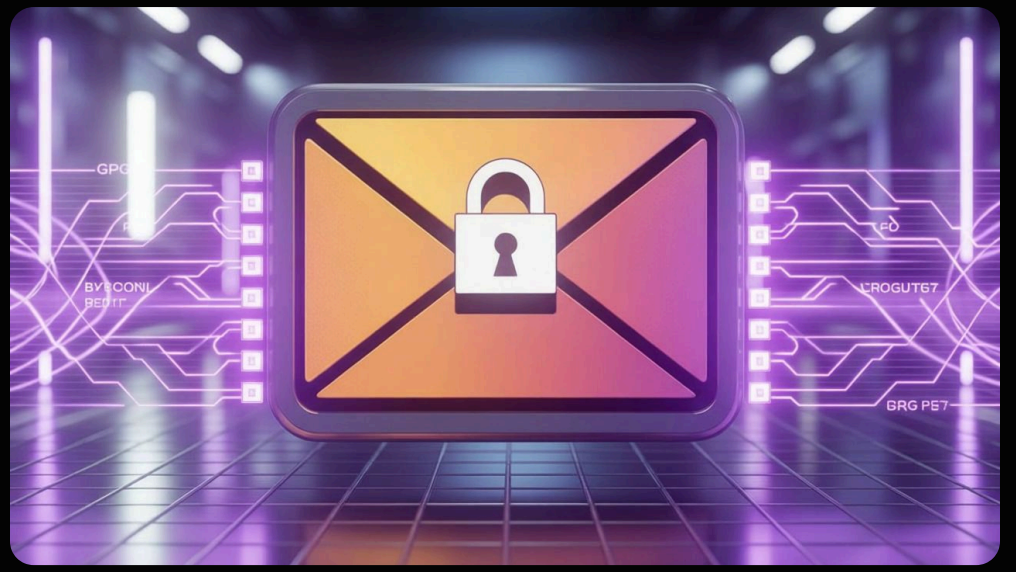
- Install Enigmail add-on
- Configure with your GPG key
- Always sign and encrypt sensitive emails

Secure Messaging

OnionShare - Share files anonymously:

```
onionshare-gui
```

Ricochet - Anonymous instant messaging over Tor (install if needed)



5. Metadata Removal

MAT2 (Metadata Anonymization Toolkit)

Remove metadata from files before sharing.

Check Metadata:

```
mat2 --show filename.pdf
```

Remove Metadata:

```
mat2 filename.pdf
```

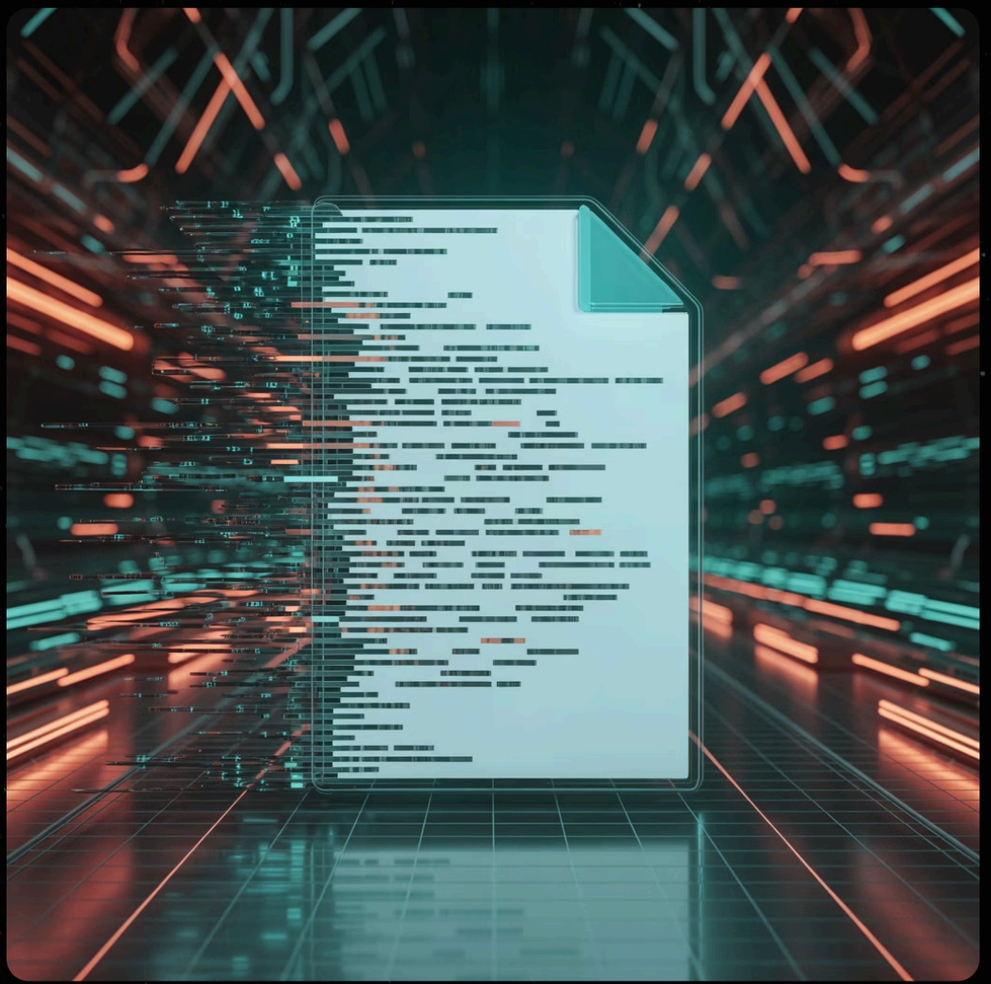
Batch Process:

```
mat2 *.jpg *.pdf *.docx
```

ExifTool

Alternative for images:

```
exiftool -all= image.jpg
```



6. VPN Configuration

Using VPN with Tor (VPN → Tor setup)

Install OpenVPN

```
sudo apt install openvpn
```

Connect to VPN

```
sudo openvpn --config your-vpn-config.ovpn
```

Then start AnonSurf

for layered anonymity:

```
sudo anonsurf start
```

⚠️ **Note**: Use trustworthy VPN providers that don't log. Consider Mullvad, ProtonVPN, or IVPN. (I use ProtonVPN Myself)

7. Best Practices

Operational Security (OpSec)

Never Mix Identities:

- Don't access personal accounts while anonymous
- Use separate devices/VMs for different identities
- Never reuse usernames across identities

Minimize Digital Footprint:

- Use disposable email addresses (guerrillamail, temp-mail)
- Create accounts with fake information
- Use cryptocurrency for payments (Monero preferred)

Traffic Analysis Protection:

- Don't torrent over Tor (use I2P instead)
- Avoid logging into sites while using Tor
- Be aware of time-zone leaks in timestamps

Physical Security:

- Use full-disk encryption
- Set BIOS password
- Enable secure boot
- Use strong passphrases, not passwords

Additional Tools in Parrot

Proxy Chains - Chain multiple proxies:

```
proxychains firefox
```

I2P - Anonymous network alternative to Tor:

```
sudo systemctl start i2p
```

Access at: http://127.0.0.1:7657

Zulucrypt - Disk encryption:

```
zulucrypt-gui
```

Quick Anonymity Checklist

Before any anonymous activity:

- MAC address randomized
- AnonSurf or VPN running
- Using Tor Browser (not regular browser)
- JavaScript disabled (if possible)
- No personal accounts logged in
- Metadata removed from files
- Using encrypted communications
- System time zone set to UTC
- WebRTC disabled
- Webcam physically covered

Testing Your Anonymity

Visit these sites to check for leaks:

- https://check.torproject.org
- https://ipleak.net
- https://browserleaks.com
- https://whoer.net

Warning

No system provides 100% anonymity. Your behavior and operational security matter more than tools. Advanced adversaries with sufficient resources may still be able to de-anonymize you through traffic analysis, timing attacks, or social engineering.

Always assume you're being monitored and act accordingly. Use anonymity tools for legitimate privacy purposes only.